# Blue green deployment

* RDS outside of beanstalk, store connection string in S3
* Use weighted routing policy

# CloudTrail

By default cloudtrail event logs are encrypted using S3 server-side encryption

If duplication events happen for cloudfront, can use AWS CLI, update cloudtrail trail to disable global service events that are delivered in all regions except US-West

# Redis Cluster

To secure:

1. Use Redis AUTH with in-transit encryption, enabled for clusters
2. VPC peering connection between 2 VPC IF ec2 and redis cluster is within same region (if not same region, use Transit VPC solution instead)

# AWS Blockchain

Any transaction between members, each member use the format:

RMN

ResourceID.MemberID.NetworkID.managedblockchain.AWSRegion.amazonaws.com:PortNumber

# AWS VPN CloudHub

VGW can be used to connect multiple locations.

Unique BGP ASN at each location

BGP peering only with VGW, not with routers in other locations

Non-overlapping IP address pool should be configured at each regional offices

# AWS Batch Job

AWS Batch Job sends log information to cloudWatch logs requires awslogs log driver configured on resource having customized AMI

# AWS Data Pipeline

Web service to automate movement and transformation of data

# CloudFront

If cache not working make sure:

1. Delimiter of query string is ‘&’
2. Check if Parameters’ names and values are in same case
3. Make sure if the distribution is a Web distribution

If use cloudFront to prevent direct access to S3, create an origin access identity (OAI) for cloudFront and grant access to the objects in S3 to that OAI.

# Amazon SQS

Smooth migration to SQS FIFO:

1. Each FIFO queue should have a Message group ID irrespective of multiple ordered message groups required
2. identical message bodies => use unique deduplication ID
3. unique message bodies => use content-based deduplication ID

# Amazon polly

Lexicons are specific for region.

If speech are too fast, do:

1. Add a pause using SSML tag between appropriate words and paragraphs
2. Convert commas into period
3. Add tag “strong” for appropriate word and paragraphs

# CloudHSM

To backup AWS CloudHSM data to S3 in same region, CloudHSM generates EBK to encrypt all data. This EBK is encrypt using Persistent backup key (PBK).

# S3

Use VPC endpoint to transfer data WITHOUT internet

VPC Gateway Endpoint for S3 and DynamoDB

**https://<bucket>.s3.amazonaws.com/<object>**

**https://s3.<region>.amazonaws.com/<bucket>/<object>**

# Kinesis Stream

VPC interface endpoint for ec2 communicate with kinesis stream without internet

Use cloudwatch monitor metrics, send notification to auto scaling, then API gateway to initiate LAMBDA function to change number of shards (CHEAPER)

Use kinesis scalint utility to modify number of shards (more expensive)

# Amazon PrivateLink

Secure and private link to ECS for control plane connectivity (or other Amazon services)

# RDS

storage volume snapshot of database instance during backup window once a day, capture transactions logs every 5 min, store in S3

# Aurora

MySQL Database engine – Aurora

15 aurora replica, across AZ and Region, less than 100 milliseconds

# DynamoDB

DYNAMODB nosql db and json, and store METADATA

Json size limit 400KB! (use EFS if is over that limit)

To transfer stale data after a week:

1. Setup DynamoDB on weekly basis, and ensure most recent week table has higher throughput
2. Use AWS data pipeline to transfer older data to S3

Use global tables for large different location, to ensure latency for data retrieval is least

Can enable autoscaling

NO READ REPLICA!!

For high read and write expectancy, use partition keys with a large number of distinct values

# Amazon Athena

Amazon Athena analyze cost and usage report uploaded in s3

Price is base upon per query and amount of data scanned in each query

# Amazon QuickSight

If need data visulaization

# IAM

Cross-account IAM roles to securely grant access to third party

# NAT and egress

NAT gateway in each AZ

NAT IS ONLY FOR IP4!

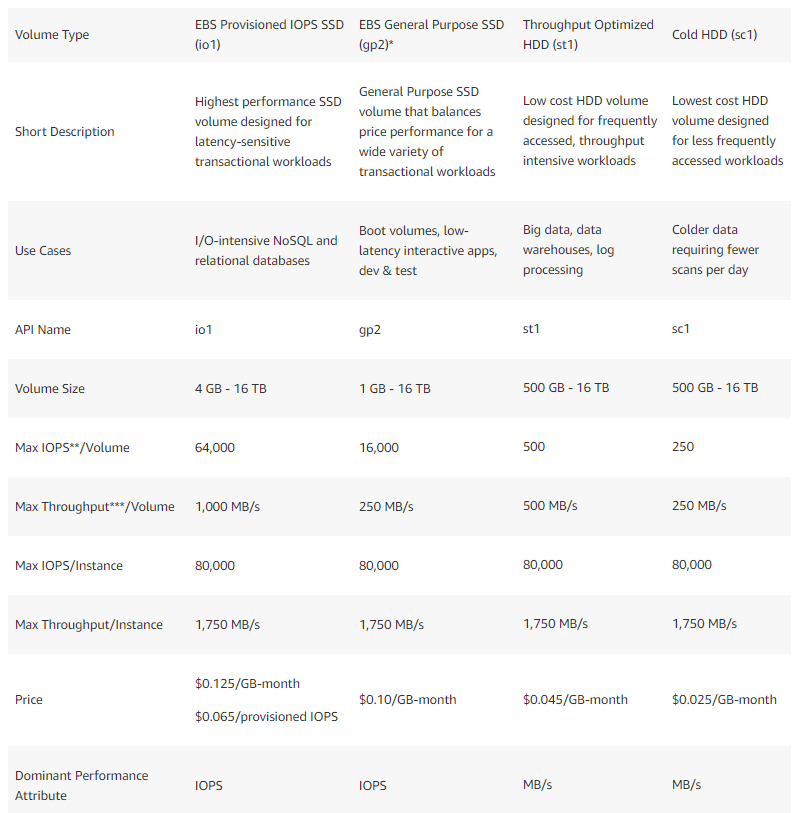
Use egress internet gateway for IP6

# Spot, on-demand, reserve instance

Spot – usually use for batch processing jobs

Reserved instances – usually for knowned longer period time

# EBS types



# AWS EFS

To enable user to save files inefs, do:

Create subdirectory for each user and grant read-write-execute permission to users. Then mount subdirectory to user’s home directory

# AWS SSO

custom permission set to set session duration min 1 hour, max 12 hours

# RED SHIFT

Amazon redshift enhanced vpc routing to transfer data WITHOUT going through internet

Redshift encryption – KMS or HSM

Free storage limit. Hence Safe cost by deleting unnecessary snapshots

Can use cloudWatch or Trusted advisor to monitor red shift performance

Can use SQL

COLUMN STORAGE

# GATEWAY CACHE AND STORED VOLUME

Cached Volumes (more for STORE DATA in AWS, cache on prem)– store in S3 and retain a copy of frequently access data locally. “minimize need of scaling on-prem storage”, “retain low-latency access to frequently access data”

Stored volumes (more for BACKUP TO AWS) – low-latency access to ALL dataset. Then asynchronous backup point-in-time snapshot to S3

# ROUTE 53

Alias – specific Route 53 extension to DNS, instead of IP address or domain name.

Alias record contains pointer to cloudFront, beanstalk, elb, S3 or another Rout3 53 record.

aname – to point whizlabs.com to IP address (whizlabs.com A 10.120.13.14)

cname with ALIAS=NO – to convert long URL to short URL

cname with ALIAS=YES – to set up a new domain to override another domain in use.

Route53 can monitor ENDPOINTS and state of cloudWatch alarm for healthcheck

# Load balancer

Application LB – allow containers to use dynamic host port mapping

Application LB supports HTTP

Network LB supports TCP/UDP

Proxy protocol for TCP/SSL carries the source (client) IP/port information

To use proxy protocol, need to confirm back-end listeners and front-end listners are configured for TCP

The proxy protocol only applies to L4 and the back-end listener must be TCP for proxy protocol

When using the proxy protocol the front-end listener can be either TCP or SSL

Without cross-zone load balancing enabled, the NLB will distribute traffic 50/50 between AZs. As there are an odd number of instances across the two AZs some instances will not receive any traffic. Therefore enabling cross-zone load balancing will ensure traffic is distributed evenly between available instances in all AZs

# Glacier retrieval time

Expedite – 1-5minutes

Vault lock and standard – 3-5 hours

Bulk – 5-12 hours

# Docker

* Suitable for batch job workloads
* Batch process app package as docker image and use ECS task
* Task definition can define:
  + Ports should be opened on container instance
  + Container image to use and repo
  + How much CPU and memory
  + If task should continue if container finish or fails
  + Command container should run when start

# Auto-scaling

If EC2 instance status is “IMPAIRED”, it means instance will be terminated, then a replacement wil be launched